RSA SECURID® ACCESS
Implementation Guide

Flatter Files

Gina Salvalzo, RSA Partner Engineering
Last Modified: June 20, 2018

RSA READY

Solution Summary

Flatter Files is a cloud based flat file cabinet for your important drawings and documents. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. Flatter Files supports user auto-provisioning.

RSA SecurID Access Features	
Flatter Files	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

The following supported use case of RSA SecurID Access with Flatter Files require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Flatter Files can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Flatter Files SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Flatter Files in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

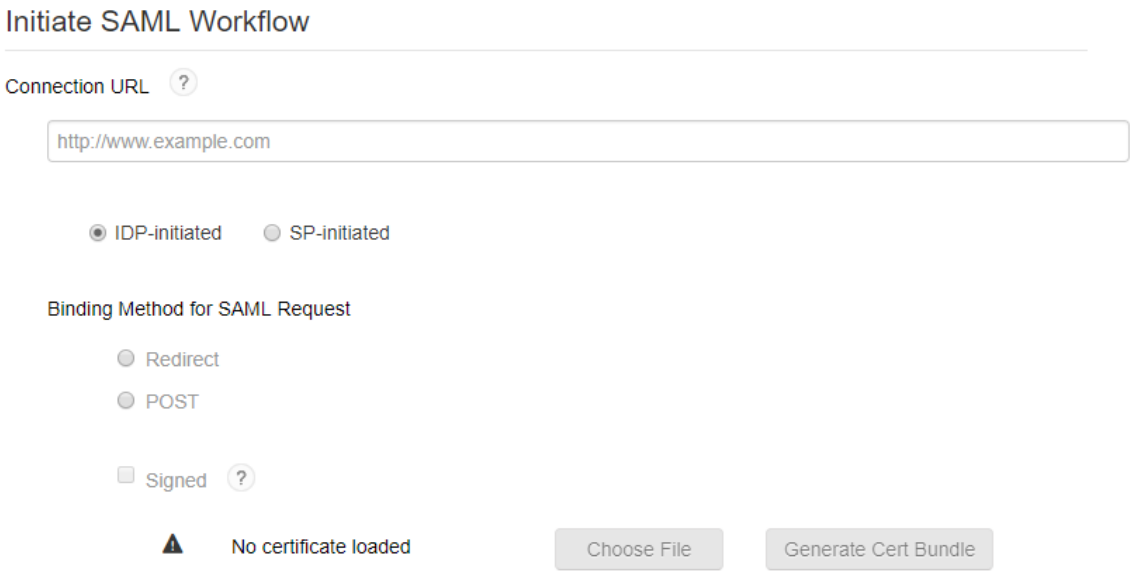
Configure RSA Identity Router SAML IdP

Procedure

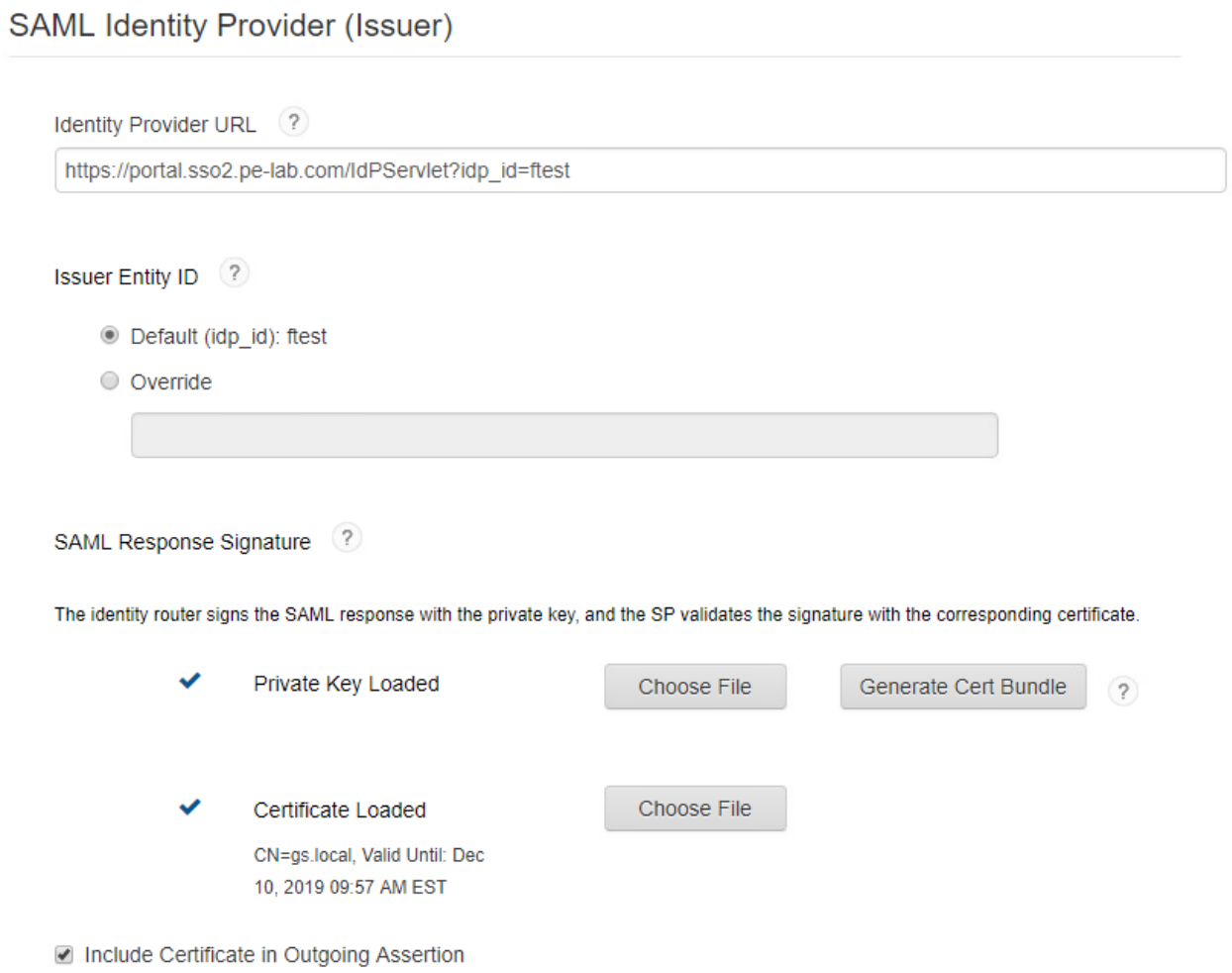
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Flatter Files and click **+Add** to add the connector.

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
   a. In the **Connection URL** field, leave the field blank.
   b. Choose **IDP-initiated.**

Note: The following IDP-initiated configuration works for SP-initiated as well.



4. Scroll down to SAML Identity Provider (Issuer) section.

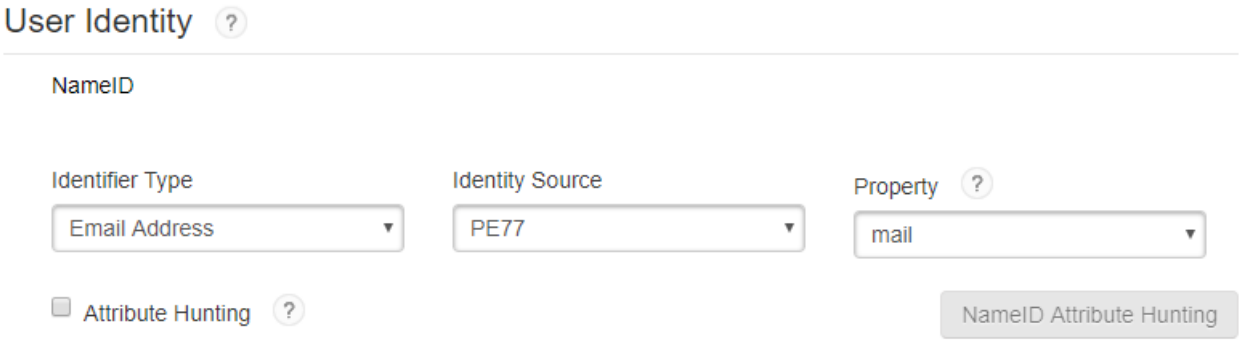


a. Make a note of Identity Provider URL value, as it will be needed later to configure the service provider configuration.
b. Select **Choose File** and upload the private key.
c. Select **Choose File** to import the public signing certificate.
d. Select the checkbox for **Include Certificate in Outgoing Assertion**.

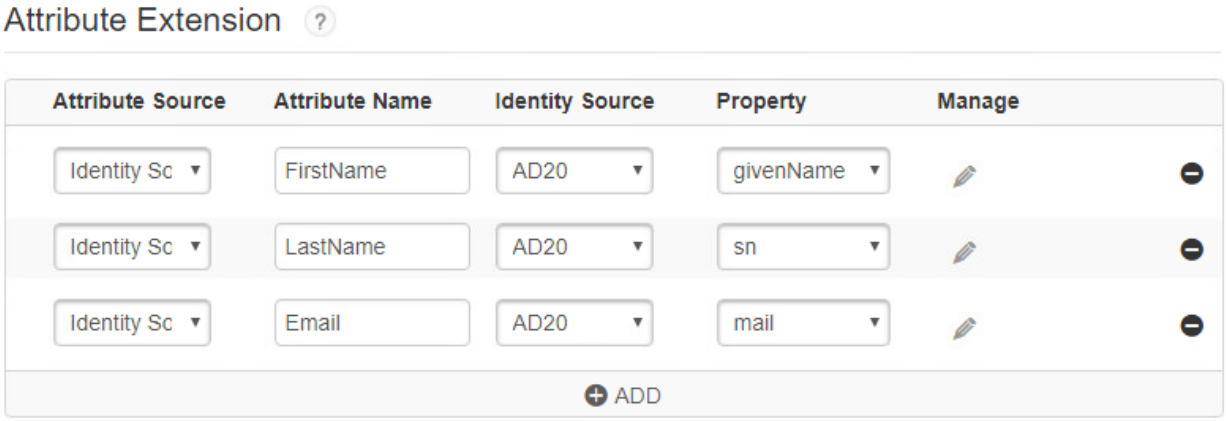
Note: The Comman Name (CN) of the certificate pair used for the assertion must match the single sign-on domain. Example: CN=pe-lab.com

5. Scroll down to the Service Provider section.

6. Verify the **Assertion Consumer Service (ACS) URL** field.
7. Verify the **Audience (Service Provider Issuer ID)** field.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

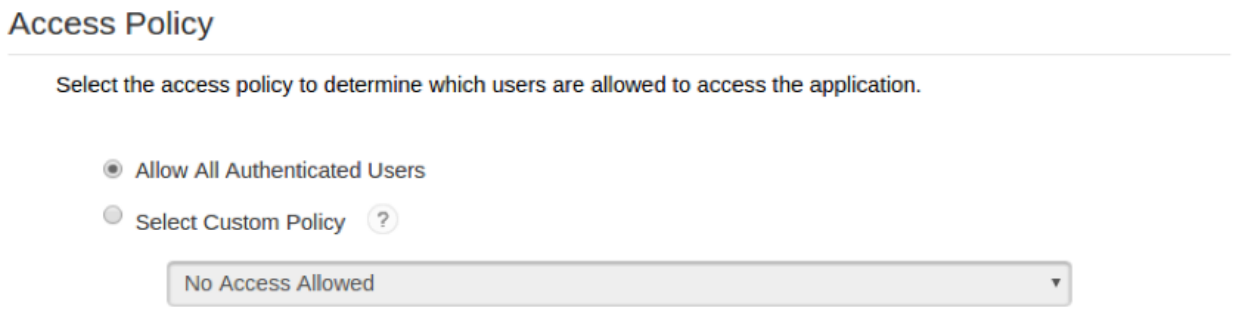


9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attributes **FirstName, LastName** and **Email** with their correlating value from your Identity source.

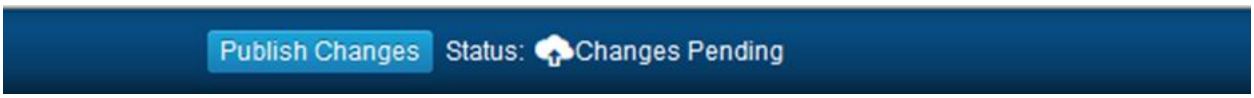


11. Click **Next Step**.

12. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



13. Click **Next Step**.
14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**. Your application is now enabled for SSO.



Partner Product Configuration

Before You Begin

This section provides instructions for configuring Flatter Files with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

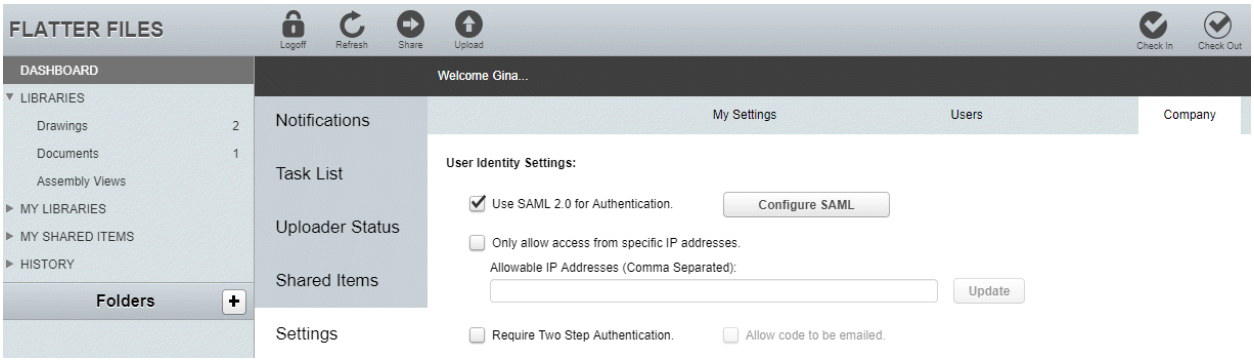
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Flatter Files components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Flatter Files SAML Configuration

Procedure

1. Contact Flatter Files support and request your domain get white listed.
2. Login to Flatter Files as an administrator. **https://www.flatterfiles.com/site/login**
3. Navigate to **DASHBOARD > Settings > Company**.
4. Check **Use SAML 2.0 for Authentication**.
5. Select **Configure SAML**.



6. In the Domain field enter the domain your requested white listed.

7. Enter the **Identity Provider URL** from step 4 on page 5.
8. Copy and paste the public certificate into the Identity Provider Certificate field without the ---BEGIN CERTIFICATE --- and --- -END CERTIFICATE--- lines.
9. Click **Update**.